CLAIMS

1. A method for restricting access to content, comprising the steps of:
embedding a biometric watermark in said content; and
providing access to a user of said content if a biometric sample of said user matches said embeddêd biometric watermark.

2. The method of claim 1, wherein said embedded biometric watermark includes a biometric image.

3. The method of claim 1, wherein said providing step further comprises the step of determining if said biometric sample is a live biometric.

4. The method of claim 1, wherein said embedded biometric watermark includes information describing a system employed by said user to obtain said content.

5. The method of claim 4, wherein said providing step further comprises the step of evaluating one or more parameters of a system employed by said user to access said content.

6. The method of claim 4, wherein said providing step further comprises the step of providing access to said content if said content is on a system that has been previously authorized for said user.

7. The method of claim 1, further comprising the step of disabling access to said content if said biometric sample of said user does not match said embedded biometric watermark.

8. A system for restricting access to content, comprising:
a memory; and

at least one processor, coupled to the memory, operative to:

embed a biometric watermark in said content; and

provide access to a user of said content if a biometric sample of said user matches said embedded biometric watermark.

9. The system of claim 7, wherein said embedded biometric watermark includes a biometric image.

10. The system of claim 7, wherein said providing step further comprises the step of determining if said biometric sample is a live biometric.

11. The system of claim 7, wherein said embedded biometric watermark includes information describing a system employed by said user to obtain said content.

12. The system of claim 10, wherein said providing step further comprises the step of evaluating one or more parameters of a system employed by said user to access said content.

13. The system of claim 10, wherein said providing step further comprises the step of providing access to said content if said content is on a system that has been previously authorized for said user.

14. The method of claim 1, wherein said processor is further configured to disable access to said content if said biometric sample of said user does not match said embedded biometric watermark.

15. An article of manufacture for restricting access to content, comprising a machine readable medium containing one or more programs which when executed implement the steps of:

embedding a biometric watermark in said content; and providing access to a user of said content if a biometric sample of said user matches said embedded biometric watermark.

16. The article of manufacture of claim 13, wherein said embedded biometric watermark includes a biometric image.

17. The article of manufacture of claim 13, wherein said providing step further comprises the step of determining if said biometric sample is a live biometric.

18. The article of manufacture of claim 13, wherein said embedded biometric watermark includes information describing a system employed by said user to obtain said content.

19. The article of manufacture of claim 16, wherein said providing step further comprises the step of evaluating one or more parameters of a system employed by said user to access said content.

20. The article of manufacture of claim 17, wherein said providing step further comprises the step of providing access to said content if said content is on a system that has been previously authorized for said user.